Cassandra Crossing/ Tor? Molto rumore per nulla

(92)—Tor funziona e offre un altissimo livello di sicurezza: gli eventi dei giorni scorsi, invece, non fanno che dimostrare come contro…

Cassandra Crossing/ Tor? Molto rumore per nulla

(92)—Tor funziona e offre un altissimo livello di sicurezza: gli eventi dei giorni scorsi, invece, non fanno che dimostrare come contro la leggerezza, o la stupidità, né la tecnologia né gli Dei possano fare alcunché.

14 settembre 2007—Martedì un dettagliatissimo articolo di *Punto Informatico* riportava in maniera puntuale ed esaustiva che Tor è stato usato come mezzo per rastrellare password in Rete e violare account di posta. Il taglio ed il tono dell'articolo suscitavano però, almeno a mio parere, allarme e sfiducia sulla capacità di garantire l'anonimato da parte della rete Tor.

Il resto di questo intervento si può perciò sintetizzare semplicemente così: "Non è vero; Tor va da Dio, purché lo si utilizzi per quello che è, non per quello che vorremmo fosse".

Sì, perché chi usa Tor da semplice utente spesso lo considera una "pallottola d'argento" che garantisce da sola l'anonimato durante la navigazione web.NON E' VERO. NON E' COSI'.

Tor è un mezzo efficace per occultare la provenienza di una connessione TCP che sta consultando e/o utilizzando un sito web. Niente di più, niente di meno. La differenza è sottile, ma abissale.

Infatti usare la rete Tor per navigare normali siti HTTP non garantisce affatto l'anonimato del navigatore, perché i dati scambiati tra il nodo Tor di uscita ed il sito web sono in chiaro.

Se si riempie un form con il proprio nome e cognome, questi dati passano in chiaro da nodo Tor di uscita, attraverso la rete di vari ISP fino al server web, e nel server web stesso. Questi tre sono punti privilegiati in cui tutte le informazioni in chiaro possono essere intercettate e memorizzate. In parole povere, se scrivete nel form il vostro nome, un nome utente od una password, il sistema dove gira il nodo Tor di uscita diventa un ideale punto di concentrazione e raccolta di informazioni personali, che passano tutte da lì per disperdersi poi nella Rete e raggiungere i server di destinazione.

Nulla garantisce che il gestore di un nodo Tor di uscita sia una persona onesta e rispettosa della privacy; puo' essere un mafioso, una spia industriale, un ladro di numeri di carta di credito, o semplicemente l'investigatore assunto dal vostro fidanzato/fidanzata per un'indagine prematrimoniale.

La rete Tor è progettata per resistere a questo, ma né Tor e **neanche gli Dei possono nulla contro la stupidaggine**.

Usare Tor e poi inviare informazioni in chiaro è appunto un'abissale stupidaggine, che rende possibile lavori dimostrativi e pubblicazioni ad effetto come quelli citati dal suddetto articolo. Facciamo ora un passo avanti.

Se vi connettete ad un servizio criptato (ad esempio un sito web HTTPS) i dati che transitano diventano ovviamente illeggibili, e solo la vostra controparte puo' leggerli. Benissimo, tutto a posto quindi. O no? Fatevi una semplice domanda.

Con chi state comunicando? Siete sicuri sia la vostra banca? Come fate a saperlo? "Beh, è semplice" direte voi "basta esaminare il certificato che il server ci invia all'inizio della sessione".

Giusto! Ma lo fate realmente? Lo fate almeno la prima volta che vi collegate? Sapete come fare a verificare un certificato solo la prima volta ed a rendere automatico il procedimento per le volte successive?

Non basta vedere che sul certificato c'è scritto "Bill Gates—Microsoft", bisogna verificarne l'autenticità tramite la catena di autorità di certificazione. Non è difficile; basta cliccare sul tasto "Dettagli" e non su "OK", solo la prima volta che l'usate.

Se invece si clicca su OK a raffica, ci si espone proprio a quello che è stato fatto (per fini dimostrativi) dal meritorio sig. Dan Egerstad.

Infatti il buon Dan ha nuovamente utilizzato il fatto che il server che ospita un nodo Tor di uscita si trova in un punto privilegiato non solo per raccogliere informazioni (come visto nel caso precedente) ma anche per tentare di alterarle "al volo".

E' quindi possibile portare un attacco di tipo MITM (Man in the Middle—Uomo nel Mezzo), che nel caso di consultazione di un sito web HTTPS (per esempio quello della vostra banca) funzionerebbe grosso modo così:

1. [il vostro browser, attraverso la rete Tor, offre un certificato e richiede quello del sito web]
2. [la richiesta esce dal nodo Tor di uscita, dove il buon Dan ha piazzato un programma proxy che intercetta la chiamata e la ferma temporaneamente]
3. [il proxy vi offre un certificato finto generato al momento, che reca informazioni ragionevoli dedotte dall'indirizzo del sito web o da quelle contenute nel vostro certificato, ma è crittograficamente falso come una moneta di latta]
4. [il vostro browser apre una finestra in cui vi chiede di approvare il certificato (taroccato) appena arrivato. Se non fate nessuna verifica e cliccate su OK il gioco è fatto.]
5. [Olè, avete appena aperto una connessione con il proxy di Dan pensando che sia il sito della vostra banca]
6. [il proxy di Dan puo' terminare l'apertura di una connessione "sicura" con voi ed usare le informazioni che gli mandate (incluso il vostro certificato) per aprire una seconda connessione da lui verso il sito della banca.]
7. [il proxy puo' poi intercettare, memorizzare e e magari anche modificare tutte le informazioni scambiate sulla connessione "sicura" ed "anonima" appena aperta. Cosa c'entra Tor in tutto questo? Assolutamente niente, ha solo offerto un punto favorevole ad un criminale per approfittare della stupidità di chi clicca sempre su "OK", persino quando vuole una connessione sicura ed anonima.]

That's all, folks. Tor funziona, e non ha debolezze conosciute; potete usarlo con fiducia. Solo usatelo per quello che è, per quello che puo fare e per come funziona, proprio come la vostra bicicletta o la vostra auto.

Concludendo: per la privacy in Rete c'è di che essere moooooooooolto preoccupati, per il funzionamento di Tor no.

Chi volesse chiarimenti può anche iscriversi alla lista e-privacy e chiederli via email.

Originally published at punto-informatico.it.

Scrivere a Cassandra—Twitter—Mastodon
Videorubrica "Quattro chiacchiere con Cassandra"
Lo Slog (Static Blog) di Cassandra
L'archivio di Cassandra: scuola, formazione e pensiero

By Marco A. L. Calamari on August 30, 2023.

Canonical link

Exported from Medium on January 2, 2024.